Quantification of Node Misbehavior in Wireless Sensor Networks: A Social Choice-Based Approach

Subarna Chatterjee* Subhadeep Sarkar‡ Sudip Misra†
*,†,‡School of Information Technology
‡School of Medical Science and Technology
Indian Institute of Technology, Kharagpur
West Bengal, India
Email: *chatterjeesubarna@yahoo.com, ‡subhadeep@smst.iitkgp.ernet.in , †smisra@sit.iitkgp.ernet.in

***Abstract*—This work focuses on the quantification of node misbehavior in wireless sensor networks (WSNs). Misbehaving nodes are common within WSNs which are once detected, are penalized and in some cases eliminated from the network. However, node misbehavior might be relative i.e., a node may exhibit maliciousness or selfishness only to a specific set of nodes and may function normally for the rest. In these cases, a complete elimination of the node from the network is unfair. This work mitigates the aforesaid problem and mathematically evaluates the extent of misbehavior of a node through the proposed *Metric of Misbehavior* (*MoM*). Based on the *Theory of Social Choice*, the proposed algorithm considers the misbehaving nodes as the voting alternatives and the normally behaving nodes as the voters. Based on majority ranking of social choice, eventually MoM is obtained for every alternative in a fair manner.**

***Index Terms*—Theory of Social Choice, Misbehavior, Quantification, Wireless sensor networks (WSNs)**

I. Background

Wireless sensor networks (WSNs) has been one of the most emerging areas of research in the recent times and it has found a widespread admissibility in many real-life fields, such as surveillance in battlefield, military systems, traffic control, health care, and biomedical applications [1], [2]. Conventionally speaking, in a WSN, nodes are embedded with sensors that are capable of sensing and monitoring certain attributes of objects or certain environmental parameters such as humidity, temperature, and air-pressure. Now, these nodes are deployed over a region forming a scattered network topology. Sensing and subsequent computations are performed on these nodes. Naturally, all algorithms, computations, and analyses are hugely dependent on sensor reading. Hence, every sensor should remain healthy throughout its lifetime in terms of its battery life, local memory, internal software, and embedded hardware performance. However, these nodes have bounded power resources, limited computation ability, and short transmission range.

Although contemporary research has found its way to improve the security issues of a WSN, current WSNs are still vulnerable to node misbehavior [3], [4]. Misbehaving or mischievous nodes violate the network protocols and subsequently lead to packet dropping, Denial of Services (DoS), decreased throughput, and reduced network lifetime. The most deadly consequences due to node misbehavior are encountered in those networks where quality of service (QoS) is of prime concern. Explored dimensions of misbehavior are stated as [5], [6],

- Accidental or deliberate- Accidental factors are the uncontrolled causative factors for misbehavior whereas the deliberate ways are the intentional reasons behind misbehavior.
- Selfish or Malicious- These refer to the programmed misbehavior from the end-user perspective.
- Individual or Collusion- These type of misbehavior generally result from individual node faults due to hardware or software failures.

Fundamental types of misbehavior of sensor nodes are mainly categorized as overloaded, selfish, malicious, and broken [7]. Overloaded nodes are those in which the local resources are excessively exhausted and are thus, incapable of processing and forwarding packets. Selfish nodes try to optimize their resource utility at the cost of total or partial dropping of packets from other nodes [8]. Malicious nodes alter the data as well as the packet format, thus destroying the integrity of the packet. Additionally, they misroute the packet or launch DoS by silently dropping packets [9]. Broken nodes suffer from software failure [7].

A. Motivation

Although existing literature have explored ways to mitigate the problem of detection of misbehaving nodes [10], [11], the true impact analysis of misbehavior has not been studied so far. This is because, unless the influence and repercussion of node misbehavior is analyzed, appropriate maneuver cannot be planned. For example, a selfish node might exhibit grey hole attack for a particular subset of nodes whereas it might be completely normal to the rest of the nodes. Also, a node can be malicious while forwarding packet to or from a particular destination. Hence, the severity of any kind of misbehavior is node-variant. Thus, the exact measure of a misbehavior can be correctly judged only from a network perspective. Since the term 'misbehavior' cannot be mathematically expressed as a measure, it leads to a blurred perception of a misbehaving node. Due to the fuzziness of the term 'misbehavior', the

978-1-4673-6305-1/15/$31.00 ©2015 IEEE

severity of it cannot be understood. Herein lies the importance of quantifying node misbehavior and subsequently arriving at a metric so that the criticality of misbehavior can be mathematically measured.

B. Contribution

In this paper, we primarily focus on deriving a metric to judge the severity of turbulence that a misbehaving node might cause to the entire WSN. Since misbehavior is a node-variant phenomenon, the perspective of each node of the network must be considered while analyzing node misbehavior. Thus, the underlying approach of this work is based on the *Theory of Social Choice*, where we view a network as a society of nodes. A measure of misbehavior is mathematically obtained by using a 'fair' voting strategy complying with the social welfare policies. This work propounds *Metric Of Misbehavior* or (*MoM*) as a magnitude of misbehavior for each node from the network point of view.

C. Organization of the paper

The rest of the paper is organized as follows. Section II depicts the system model and the details of the implementation of the theory of social choice. The performance evaluation is presented in Section III in which the quantification of misbehavior is thoroughly analyzed. Finally, Section IV concludes the work and discusses the future scopes of the work.

II. System Model

This Section presents the detailed aspects of our model based on the *Theory of Social Choice*. We consider a WSN consisting of a set $\mathcal{N}$ of n number of sensor nodes, $\mathcal{N} = \{N_1, N_2, \ldots, N_n\}$. We assume that, based on some standard existing misbehavior detection algorithms [9], [10], [12], a set $\mathcal{M}$ of m number of misbehaving nodes has been reported, $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$. So, $\mathcal{M} \subseteq \mathcal{N}$. $\mathcal{N}$ is the set of voters and $\mathcal{M}$ is the set of alternatives. We also assume the topology of the WSN to be a clustered one [13], [14]. For our simplicity, we present the details of our approach for a single cluster. However, the same algorithm can be made applicable to multiple clusters by simultaneous execution of this algorithm in every clusters of the network.

Modern *Theory of Social Choice* is based on Arrow's Impossibility Theorem. Economic systems, interpret the theorem as an event of impossibility while executing voting strategies, i.e., if a system has atleast three alternatives and atleast two voters, no democratic procedure can simultaneously satisfy Pareto axiom (P) and Independence of Irrelevant Alternatives (IIA) [15], to be discussed later. In this work, it is realistic to consider $n \gg 2$ and $m \gg 3$.

Initially, the set $\mathcal{N}$ forms a society and each member evaluates the members of $\mathcal{M}$. A particular node N_i judges a misbehaving node M_j and assigns a score to it $\theta_{i,j}$. Based on the combined preferences of each node N_i, we propose a measure of misbehavior called *Metric of Misbehavior (MoM)* for each misbehaving node M_j.

A. States of nodes

Suppose, node N_i has transmitted $\mathcal{I}_{i,j}$ number of packets to node M_j. $O_{i,j}$ out of $\mathcal{I}_{i,j}$ number of packets are further transmitted by M_j, Also, let us assume that, $S_{i,j}$ number of packets transmitted by N_i were destined for M_j. We have,

$$O_{i,j} \geq 0, S_{i,j} \geq 0, \forall N_i \in \mathcal{N}, \forall M_j \in \mathcal{M} \tag{1}$$

We now define packet drop rate γ of M_j with respect to N_i as:

$$\gamma_{i,j} = \frac{\mathcal{I}_{i,j} - O_{i,j} - S_{i,j}}{\mathcal{I}_{i,j} - S_{i,j}} \tag{2}$$

直接Gaussian分布？ 假设太强烈了...

γ ranges from 0 to 1 and is assumed to follow a symmetrical Gaussian distribution $f(\gamma)$. Hence, mean (μ) is 0.5. The standard deviation σ is allowed to vary within 3 times of it as per the 3-sigma rule. A wider range of standard deviation considers a broader possibility of misbehavior. This reduces the probability of not considering misbehaving nodes. From the 3-sigma rule, we already have,

3-sigma规则

$$\int_{\mu-\sigma}^{\mu+\sigma} f(\gamma)\, d\gamma = 0.68 \tag{3}$$

From this it follows,

$$\int_{\mu}^{\mu+\sigma} f(\gamma)\, d\gamma \simeq 0.34 \tag{4}$$

This is because only a decreased deviation from μ is irrelevant for assessment of misbehavior as it reduces the rate of dropping packets. Thus, we only consider deviation towards the positive X axis. We introduce network modeled thresholds d_1, d_2 and d_3. $d_1 = 0.34$. Similarly,

$$d_2 = \int_{\mu+\sigma}^{\mu+2\sigma} f(\gamma)\, d\gamma \simeq 0.13 \tag{5}$$

$$d_3 = \int_{\mu+2\sigma}^{\mu+3\sigma} f(\gamma)\, d\gamma \simeq 0.02 \tag{6}$$

From the network threshold values, we may arrive at different state of nodes as stated below.

i. *Safe*- These nodes have a very low probability of dropping packets and are generally among the normally behaved nodes of the network.
ii. *Unsafe*- These nodes have a moderate probability of dropping packets i.e, they might have dropped packets due to traffic congestion or due to some temporary software fault. They might also be partially misbehaving to the network. Hence, they are not completely worthy of blame. *Unsafe* nodes may result in grey hole attack.
iii. *Immoral*- These nodes are extremely harmful as the have a high rate of dropping packets due to maliciousness or selfishness or over-burdening.
iii. *Dead*- These nodes almost stop participating from network activities. Broken nodes can be viewed as *dead* nodes due to the lack of potential of forwarding packets.

We mathematically define the different state of nodes in our system. Figure 1. depicts the state of nodes in the range of various standard deviations.

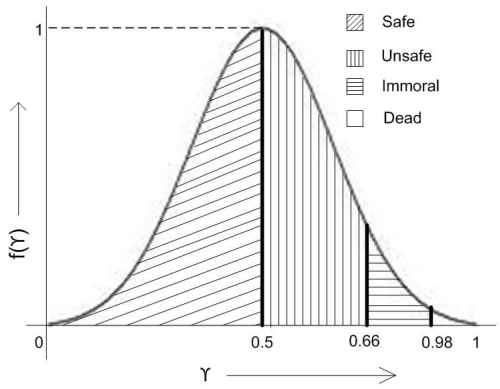


Fig. 1: Impact of γ on the state of nodes

Definition 1. A node N_i is judged as a *safe* node by node M_j, if its packet drop rate is sufficiently low, i.e.,

$$\gamma_{j,i} < \mu \tag{7}$$

A *safe* node negatively deviates from the Gaussian mean of the packet drop rate, γ.

Definition 2. A node N_i is judged as a *unsafe* node by node M_j, if its packet drop rate is moderately high, i.e.,

$$\mu \geq \gamma_{j,i} > \mu + d_1 \tag{8}$$

An *unsafe* node positively deviates from its Gaussian mean within unit standard deviation.

Definition 3. A node N_i is judged as a *immoral* node by node M_j, if its packet drop rate is sufficiently high, i.e.,

$$\mu + d_1 \geq \gamma_{j,i} > \mu + d_1 + d_2 \tag{9}$$

An *immoral* node positively deviates from its Gaussian mean within twice the standard deviation.

Definition 4. A node N_i is judged as a *dead* node by node M_j, if its packet drop rate is very close to unity. We have,

$$\mu + d_1 + d_2 \geq \gamma_{j,i} > \mu + d_1 + d_2 + d_3 \tag{10}$$

A *dead* node positively deviates from its Gaussian mean within thrice the standard deviation.

B. Computation of Power Slag

We introduce a new term to measure the energy dissipation rate of a sensor node. It is the *Power Slag* (ξ) of a node. ξ is expressed as follows.

$$\xi_i = \frac{E_{cur,i}}{E_{act,i}} \tag{11}$$

where, E_{act} and E_{cur} are the initial and current levels of energy of node i, respectively. We assume that E_{act} is known at the time of deployment and a node is capable of measuring its current power level E_{cur}. ξ of a node is highly significant as it contributes directly to selfishness or maliciousness. In this work we use ξ as a multiplicative factor in the rate of packet dropping.

C. Individual Preferences of nodes

After each node $N_i \in \mathcal{N}$ computes $\gamma_{i,j}$ for each node $M_j \in \mathcal{M}$, we obtain a score matrix Θ for the entire network as follows.

$$\Theta = \begin{bmatrix} \xi_1 \times \gamma_{1,1} & \xi_2 \times \gamma_{1,2} & \cdots & \xi_m \times \gamma_{1,m} \\ \xi_1 \times \gamma_{2,1} & \xi_2 \times \gamma_{2,2} & \cdots & \xi_m \times \gamma_{2,m} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \xi_1 \times \gamma_{n-m,1} & \xi_2 \times \gamma_{n-m,2} & \cdots & \xi_{n-m} \times \gamma_{n-m,m} \end{bmatrix}$$

Substituting, $\theta_{i,j} = \xi_j \times \gamma_{i,j}$, $\theta \in \mathbb{R}$ we get,

$$\Theta = \begin{bmatrix} \theta_{1,1} & \theta_{1,2} & \cdots & \theta_{1,m} \\ \theta_{2,1} & \theta_{2,2} & \cdots & \theta_{2,m} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \theta_{n-m,1} & \theta_{n-m,2} & \cdots & \theta_{n-m,m} \end{bmatrix}$$

Every node N_i of the network prepares its own set of preferences. We define the key terminologies of the *Theory of Social Choice* with respect to our model.

Definition 5. A binary relation P_i of a voter N_i between two misbehaving nodes M_a and M_b is a *preference* if it is anti symmetric and transitive. aP_ib should satisfy the following:

$$\theta_{i,a} > \theta_{i,b}, \forall N_i \in \mathcal{N}, \forall M_a, M_b \in \mathcal{M} \tag{12}$$

For transitivity of preference, we have,

$$aP_ib,\ bP_ic \Rightarrow \theta_{i,a} > \theta_{i,b} > \theta_{i,c}, \forall i \in \mathcal{N}, \forall M_a, M_b \in \mathcal{M} \tag{13}$$

Definition 6. A binary relation I_i between two nodes a and b is an *indifference* if it is symmetric and transitive. aI_ib should satisfy the following:

$$\theta_{i,a} = \theta_{i,b}, \forall N_i \in \mathcal{N}, \forall M_a, M_b \in \mathcal{M} \tag{14}$$

For transitivity of indifference, we have,

$$aI_ib,\ bI_ic \Rightarrow \theta_{i,a} = \theta_{i,b} = \theta_{i,c}, \forall N_i \in \mathcal{N}, \forall M_a, M_b \in \mathcal{M} \tag{15}$$

$$aI_ib,\ bP_ic \Rightarrow \theta_{i,a} > \theta_{i,c}, \theta_{i,b} > \theta_{i,c}, \forall N_i \in \mathcal{N}, \forall M_a, M_b \in \mathcal{M} \tag{16}$$

For every node $M_i \in \mathcal{M}$, a preference set is obtained from matrix Θ as $\{\theta_{1,i}, \theta_{2,i}, \ldots, \theta_{n-m,i}\}$. A weak preference ordering R_i of a misbehaving node node $\mathcal{M}_i$ is defined as the ordering that may contain both strict preferences and

indifferences. Thus, from the preference set, a weak ordering of preferences is obtained for each member of $\mathcal{M}$ as,

$$R_i = \hat{\theta}_{1,i}, \hat{\theta}_{2,i}, \ldots, \hat{\theta}_{n-m,i} \tag{17}$$

The property of $\hat{\theta}$ [1] are:

- *Property 1:* $\hat{\theta}_{j,i} > \hat{\theta}_{k,i}$, if $j < k$, $\forall i, j, k \in \mathbb{N}$
- *Property 2:* $\hat{\theta}_{j,i} = \hat{\theta}_{k,i} \Rightarrow j = k$, $\forall i, j, k \in \mathbb{N}$
- *Property 3:* $\hat{\theta}_{j+1,i} \not\Rightarrow \theta_{j+1,i}$, $\forall i, j, k \in \mathbb{N}$

Definition 7. A preference profile $\mathcal{P}$ is defined as the set of possible potential preference orderings, i.e.,

$$\mathcal{P} = \{R_1, R_2, \ldots, R_m\} \tag{18}$$

D. Collective node preference

Having defined a preference profile $\mathcal{P}$, we proceed to introduce our social choice function (SCF). Initially, we have an order function defined as $f : \mathbb{R}^n \Rightarrow \mathbb{R}$. f accepts a weak ordering of a misbehaving node as input.

In this work, we define the SCF as a function $F : \mathcal{P}^n \Rightarrow M!$, i.e., from the preference domain, we derive any possible permutation of m nodes. We have,

$$F(R_1, R_2, \ldots, R_n) = \{\hat{M}_1, \hat{M}_2, \ldots, \hat{M}_m\} \tag{19}$$

Now,

$$F(\mathcal{P}) = F_1(f(\mathcal{P}))$$

$$\text{or, } F(f(\hat{\theta}_{1,1}, \hat{\theta}_{2,1}, \ldots, \hat{\theta}_{n-m,1}), \ldots, f(\hat{\theta}_{1,m}, \hat{\theta}_{2,m}, \ldots, \hat{\theta}_{n-m,m})) = \{\hat{M}_1, \hat{M}_2, \ldots, \hat{M}_m\} = \hat{\mathcal{M}} \tag{20}$$

k^{th} order of f, denoted by f^k is defined as the k^{th} highest value of θ. f^k of a node N_i is expressed as,

$$f_i^k(\hat{\theta}_{1,i}, \hat{\theta}_{2,i}, \ldots, \hat{\theta}_{n-m,i}) = \hat{\theta}_{k,i} \tag{21}$$

Now, we denote f^{med} is the median order of f. For the purpose of maintaining simplicity, we use $f_i^{med}(\cdot)$ instead of $f_i^{med}(\hat{\theta}_{1,i}, \hat{\theta}_{2,i}, \ldots, \hat{\theta}_{n-m,i})$

中位值；奇数个
两个中位数的均值；偶数个

$$f_i^{med}(\cdot) = \begin{cases} f_1, & \text{when } n-m \text{ is odd} \\ f_2, & \text{otherwise} \end{cases} \tag{22}$$

e,

$$f_1 = \hat{\theta}_{(n-m+1)/2,i} \tag{23}$$

$$f_2 = \frac{\hat{\theta}_{\frac{n-m}{2},i} + \hat{\theta}_{\frac{n-m}{2}+1,i}}{2} \tag{24}$$

Thus, Equation (22) reduces to,

$$F_1(f_1^{med}(\cdot), f_2^{med}(\cdot), \cdots, f_m^{med}(\cdot)) = \hat{\mathcal{M}} \tag{25}$$

[1]Applying the properties below, any vector $V = \{v_1, v_2, \ldots, v_n\}$ can be converted to $\hat{V} = \{\hat{v}_1, \hat{v}_2, \ldots, \hat{v}_n\}$. Henceforth, such conversions will be directly referenced, without casting mathematical details.

Now, for the median order value of particular node M_i, we define π_1 and π_2 as the number of nodes who have voted for M_i with a score less than $f_i^{med}(\cdot)$ and greater than $f_i^{med}(\cdot)$, respectively. Thus,

$$\pi_{1,i} = |j| : \theta_{j,i} < f_i^{med}(\cdot), \forall N_j \in \mathcal{N} \tag{26}$$

$$\pi_{2,i} = |j| : \theta_{j,i} > f_i^{med}(\cdot), \forall N_j \in \mathcal{N} \tag{27}$$

We define a majority grade [16] (μ^*) from a triplet (μ^-, μ^o, μ^+).

$$\mu_i^* = \begin{cases} \mu^- & : \pi_1, i > \pi_2, i \\ \mu^o & : \pi_1, i = \pi_2, i \\ \mu^+ & : \pi_1, i < \pi_2, i \end{cases} \tag{28}$$

We express the majority grade in the form of ($\pi_{1,i}$, μ_i^*, $\pi_{2,i}$).

E. Tie-handling in majority ranking

Handling of ties is very significant in a collective preference. Under no circumstance, two nodes can be identically quantified with respect to their misbehavior. Majority grade of node M_i wins over node M_j, if the following equation holds.

$$\mu_i^* > \mu_j^* \Leftrightarrow (\pi_{1,i}, \mu_i^*, \pi_{2,i}) > (\pi_{1,j}, \mu_j^*, \pi_{2,j}) \tag{29}$$

$$\text{Also, } (\mu_i > \mu_j) \wedge (\mu_i^+ > \mu_i^o > \mu_i^-) \Leftrightarrow \mu_i^* > \mu_j^* \tag{30}$$

The condition of a tie between two nodes occurs when $\mu_i^* = \mu_j^*$. To break the tie, we apply to check whether $(\pi_{1,i}, \mu_i^+, \pi_{2,i}) > (\pi_{1,j}, \mu_j^+, \pi_{2,j})$ [16]. We need to have either of the following conditions:

$$\pi_{1_i} > \pi_{1_j} \tag{31}$$

j评价更低

$$(\pi_{1,i} = \pi_{1,j}) \wedge (\pi_{2,i} < \pi_{2,j}) \tag{32}$$

A tie on the value of μ_i^+ is resolved with μ_i^-. For this we must have, either of the following.

$$\pi_{2,i} < \pi_{2,j} \tag{33}$$

j评价更低

$$(\pi_{2,i} = \pi_{2,j}) \wedge (\pi_{1,i} > \pi_{1,j}) \tag{34}$$

Similarly, if $\mu_i^- = \mu_j^-$, we must have either of,

$$\pi_{2,i} < \pi_{2,j} \tag{35}$$

$$(\pi_{1,i} = \pi_{2,i}) \wedge (\pi_{1,j} > \pi_{2,j}) \tag{36}$$

F. Metric of Misbehavior (MoM)

The output of the SCF, $F(\cdot)$, is a linear ordering $\hat{M}$ of m misbehaving nodes. The ordering suggests the criticality of misbehavior in the decreasing order. After obtaining the ordering, for each node M_i, the metric of misbehavior *MoM*, denoted by $\Psi(M_i)$, is computed as follows:

$$\Psi(M_i) = \frac{\Gamma_i f_i^{med}(\cdot)\rho(M_i)}{\sum_{j=1}^{m} \Gamma_j f_j^{med}(\cdot)\rho(M_j)} \quad (37)$$

where $\rho(M_i)$ is the positional rank of the misbehaving node, M_i, in $\hat{\mathcal{M}}$, and Γ_i is the mean packet drop rate of the node M_i, computed as $\Gamma_i = \frac{\sum_{j=1}^{n-m} \gamma_{j,i}}{n-m}$.

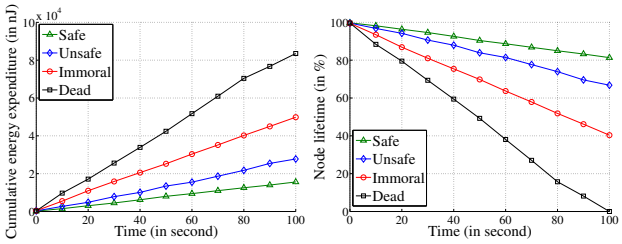
III. Performance Evaluation

The Section illustrates the details of the experimental setup, and the corresponding results obtained. We observe the effects of the presence of different types of node (viz. safe, unsafe, immoral, and dead) in the vicinity of the normally behaving nodes in terms of its energy drainage and lifetime. We also project the impact of the mean packet drop rate (Γ_i) and the residual power (ξ_i) on the MoM (Ψ_i) value of misbehaving nodes. The experimental setup is described in tabular format as follow:

TABLE I: Experimental Setup

Parameters	Values
Deployment area	1000 m × 1000 m
Deployment type	Uniform, random
Number of nodes	100
Communication range	150 m
Communication energy	20 nJ/bit
Sensing energy	10 nJ/event
Processing energy	5 nJ/bit

We consider a uniform random deployment of the sensor nodes over an 1000m X 1000m even terrain, and the nodes are assumed to follow multi-hop communication protocol within the network. In Figure 2, the effect of the presence of different types of next-hop neighbor nodes are analyzed from the perspective of a normal transmitting node. As shown in Figure 2(a), in presence of misbehaving nodes the energy depletion varies with the state of the node. The figure clearly indicates that while transmitting data packets to a safe next-hop node, the cumulative energy consumption increases marginally with time. In presence of unsafe and immoral neighboring nodes the energy depletion rates are observed to be comparatively high due to large packet drop and successive retransmissions. In case of dead nodes, however, as the mean packet drop rate (Γ_i) tends to unity, the sender node ends up in huge number of retransmissions for successful delivery of a data-packet, which in turn, yields in significantly high rate of energy consumption. Consequently, as shown in Figure 2(b), the lifetime of a sender node varies in coherence with its energy depletion rate. It is indicative that the lifetime of a node is highly affected by the presence of misbehaving nodes in the vicinity of a normally behaving node. The lifetime of a node with only safe neighbor nodes is, in fact, observed to be almost 5 times more than that of a node with dead neighbor nodes only.



(a) Energy consumption vs time (b) Node lifetime vs time

Fig. 2: Impact of presence of different types of neighbor nodes

To analyze the impact of the contributing factors on the magnitude of MoM, we perform an experiment for 100 iterations. We consider a network of 100 nodes out of which 5% are considered to be misbehaving. At every iteration the network is subjected to a static set of misbehaving nodes as the social choice alternatives, and based on the decisions of the voters the misbehaving nodes are ranked and the corresponding MoMs are computed. Figure 3 depicts the state of the alternatives of the society in terms of the mean packet drop rate (Γ_i), residual power (ξ_i), and the MoM (Ψ_i) $\forall i \in \mathcal{M}$ after different time-intervals (number of iterations). As a case study, we first observe the misbehaving node with ID 1. It is noticed that the value of Γ_1 remains almost unaltered in this case, and with the decrease of ξ_1 over time, the magnitude of Ψ_1 decreases linearly. Therefore, it is derived that for constant value of Γ_i, the Ψ_i bears a direct proportionality with ξ_i. On the other hand, for the misbehaving node with ID 3, comparing Figure 3(b) and Figure 3(c), we observe that although ξ_3 decreases steadily with time, as the value of Γ_3 increases, Ψ_3 also follows an increasing trend. Therefore, it can be fairly concluded that the effect of mean packet drop rate on the MoM is considerably higher than that of residual power.

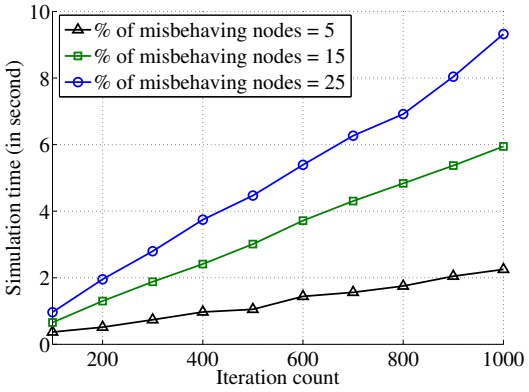
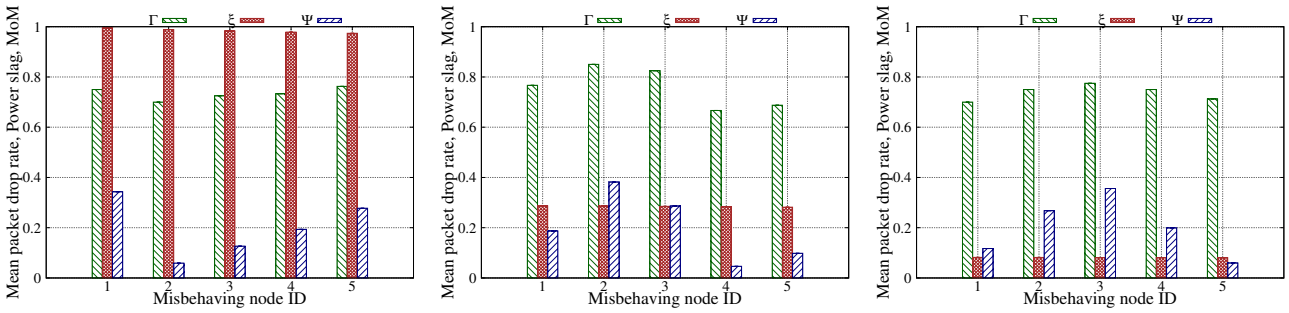


Fig. 4: dd

For the sake of complexity analysis of the proposed algorithm, we consider the execution time of the simulations as



(a) After 1 iteration (b) After 50 iterations (c) After 100 iterations

Fig. 3: Analysis of MoM with the variation of mean packet drop rate and residual power

a metric for evaluating the computational complexity of the algorithm for obtaining MoM. Figure 4 indicates the variation of the simulation time with the increase in the number of iterations. It is clearly observed that the simulation time is reasonably low when the 5% nodes of the network are misbehaving. When the percentage of such nodes is increased to 10, the algorithmic complexity increases. However, the increase in the running time is reasonable high with 25% misbehaving nodes. This is because the increase in the number of social choice alternatives, necessitates the generation of weak orderings of larger length by the voters of the society. It is observed that even for a network comprising of 25% misbehaving nodes, the computational time per iteration per node approximates to 0.01 second. Therefore, the real-time processing ability of the proposed algorithm is inferred.

IV. Conclusion

This work addresses the quantification of a node misbehavior from a network point of view. In this work, we assume the entire WSN to form a society comprising of the normally behaving nodes as the voters and the misbehaving nodes as the alternatives. Thereby, we implement the majority ranking of the theory of social choice to arrive at a fair evaluation of MoM for every alternatives. In future, the work can be extended and analyzed on a real sensor network. Further, the work can be studied for a wider range of network parameters to maintain the Quality of Service (QoS) of a WSN.

References

[1] Y.-X. Li, L.-B. Lu, and D.-Y. Liu, "Research on battlefield target tracking in wireless sensor networks," in 2^{nd} *International Workshop on Database Technology and Applications (DBTA)*, November 2010, pp. 1–4.

[2] R. A. Rashid, M. R. A. Rahim, M. A. Sarijari, and N. Mahalin, "Design and implementation of wireless biomedical sensor networks for ECG home health monitoring," in *International Conference on Electronic Design*, December 2008, pp. 1–4.

[3] F. Xing and W. Wang, "On the survivability of wireless ad hoc networks with node misbehaviors and failures," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, pp. 284–299, July 2010.

[4] L. Guang, C. Assi, and A. Benslimane, "Mac layer misbehavior in wireless networks: challenges and solutions," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 6–14, Aug 2008.

[5] A. Dadhich, A. Sarje, and K. Garg, "A distributed cooperative approach to improve detection and removal of misbehaving manet nodes," in *3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE*, January 2008, pp. 728 – 735.

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 22–32, Jan 2014.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in 6^{th} *International Conference On mobile Computing and Networking, MOBICOM*, 2000, pp. 255–265.

[8] H. Liu, J. G. Delgado-Frias, and S. Medidi, "Using a cache scheme to detect misbehaving nodes in mobile ad-hoc networks," in 15^{th} *IEEE Intl. Conf. on Netw., ICON*, November 2007, pp. 7 – 12.

[9] T. Manikandan and K. Sathyasheela, "Detection of malicious nodes in manets," in *IEEE International Conference on Communication Control and Computing Technologies (ICCCCT)*, October 2010, pp. 788 – 793.

[10] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Distributed detection in wireless sensor networks in the presence of misbehaving nodes," in *Military Communications Conference, MILCOM*, November 2012, pp. 1–6.

[11] A. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 6, pp. 1124–1134, August 2007.

[12] D. McCoy, D. Sicker, and D. Grunwald, "A mechanism for detecting and responding to misbehaving nodes in wireless networks," in $4th$ *Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, June 2007, pp. 678 – 684.

[13] Y. Liao, H. Qi, and W. Li, "Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks," *IEEE Sensors Journal*, vol. 13, no. 5, May 2013.

[14] J.-S. Kim, S.-Y. Choi, S.-J. Han, J.-H. Choi, J.-H. Lee, and K.-W. Rim, "Alternative cluster head selection protocol for energy efficiency in wireless sensor networks," in *Software Technologies for Future Dependable Distributed Systems, 2009*, March 2009, pp. 159 – 163.

[15] D. Polett, "Empowering the voter: A mathematical analysis of borda count elections with non-linear preferences," The Division of Science, Mathematics, and Computing of Bard College, Tech. Rep., May 2010.

[16] M. Balinski and R. Laraki, "Election by majority judgement: Experimental evidence," *Centre National De La Recherche Scientifique*, vol. 1, February 2008.